



FortiAuthenticator v3.1, FortiOS v5.2.0, and
Windows 7 SP1
Wireless EAP-TLS Configuration



FortiAuthenticator v3.1, FortiOS v5.2.0, and Windows 7 SP1 Wireless EAP-TLS Configuration
June 25, 2014

Copyright© 2014 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Technical Documentation	docs.fortinet.com
Fortinet Video Library	video.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Contents

Introduction	4
Audience	4
Prerequisites	4
FortiAuthenticator	4
Creating a Local CA	4
Creating a Local Services Certificate	7
Configuring RADIUS-EAP on FortiAuthenticator	9
Configuring RADIUS Client on FortiAuthenticator	10
Configuring Local User on FortiAuthenticator	11
Configuring End User Certificates on FortiAuthenticator	12
FortiGate	14
Creating RADIUS Client on FortiOS	14
Creating WiFi SSID on FortiGate	15
Windows 7 PC Configuration	16
Exporting certificate from FortiAuthenticator	16
Importing certificate into Windows 7	18
Configuring Wireless Profile to use Certificate	21
Appendix A: Verifying Login via FortiAuthenticator Logs	24

Introduction

The purpose of this guide is to provide a known working configuration of wireless client authentication using certificates via the EAP-TLS authentication method. This guide will specifically focus on the configuration of the FortiAuthenticator, FortiGate and Windows 7 needed to get this access to function.

Audience

This guide is written for network administrators who understand the following concepts:

1. FortiOS
2. FortiAuthenticator
3. EAP-TLS

Prerequisites

1. FortiAuthenticator 3.1 GA
2. FortiOS 5.2
3. Windows 7 SP1 (with support for EAP-TLS)

FortiAuthenticator

Creating a Local CA

In this environment, the FortiAuthenticator will act as the sole certificate authority for all certificates authenticated for client access. To enable this functionality on the FortiAuthenticator, a self-signed root CA certificate must be generated. This can be done via the following steps:

1. Log into the FortiAuthenticator via the webGUI
2. Navigate to "Certificate Management | Certificate Authorities | Local CAs"

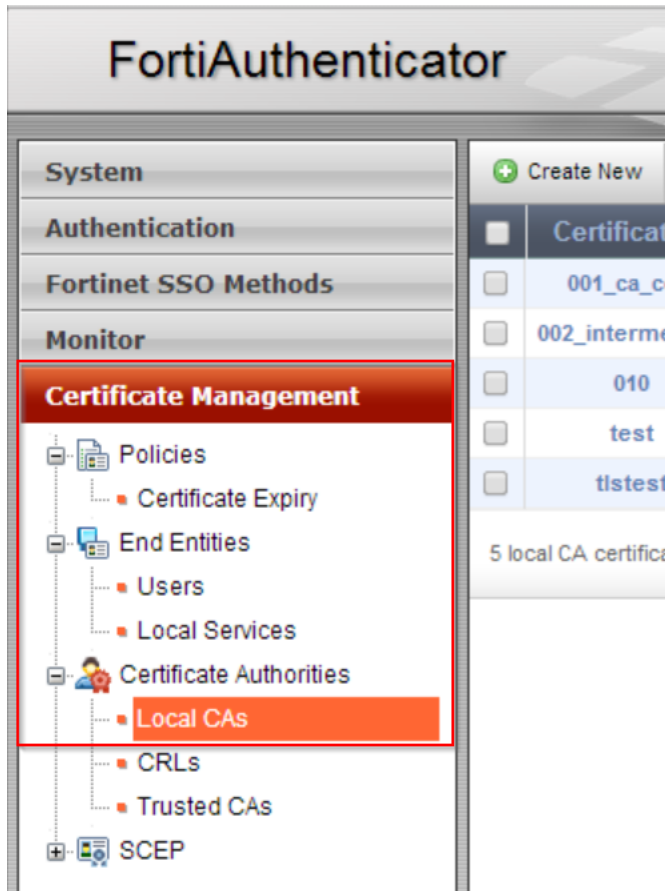


Figure 1. – Screenshot of Local CAs section in FortiAuthenticator

3. Click “Create New”

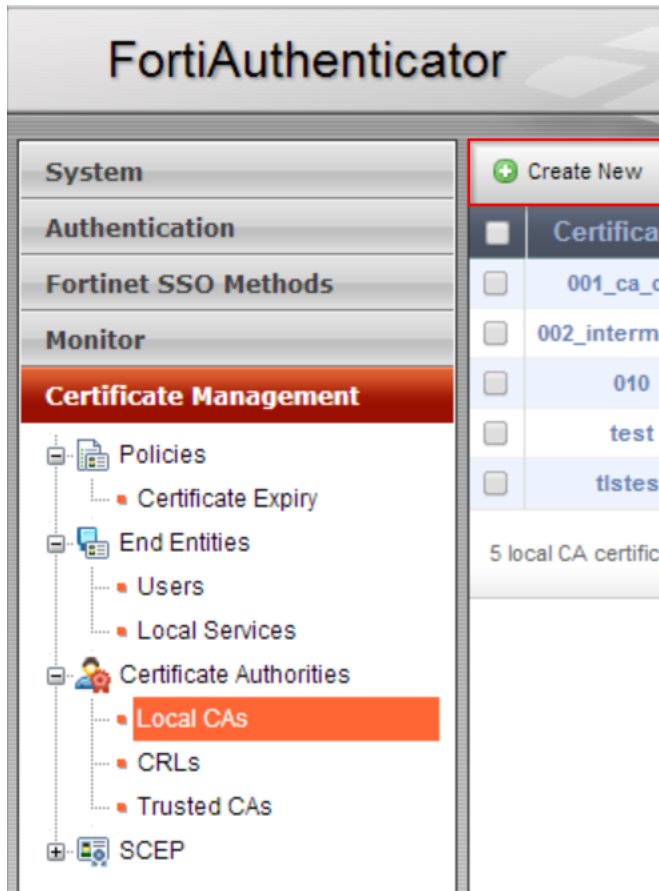


Figure 2. – Screenshot of “Create New” button in FortiAuthenticator

4. Complete the information in the fields pertaining to your organization (example in screenshot below)

The screenshot shows the 'Create New' form for a Certificate Authority in FortiAuthenticator. The form is titled 'Certificate ID: rootCA'. It has several sections:

- Certificate Authority Type:** Certificate type: ☒ Root CA certificate ☐ Intermediate CA certificate ☐ Intermediate CA certificate signing request (CSR)
- Subject Information:** Subject input method: ☒ Fully distinguished name ☐ Field-by-field. Fields include: Name (CN): FortiAuthenticator, Department (OU): Information Technology, Company (O): Local Company, City (L): Somewhere, State/Province (ST): Virginia, Country (C): United States (US) (dropdown), and Email address: admin@localcompany.c
- Subject Alternative Name:** Email: (empty field), User Principal Name (UPN): (empty field)
- Additional Options:** Validity period: ☒ Set length of time ☐ Set an expiry date. Fields include: 3650 days, Key type: RSA, Key size: 2048 Bits (dropdown), and Hash algorithm: SHA-1 (dropdown).

 The left navigation menu is visible, with 'Local CAs' highlighted. The top right shows 'Logged in as admin' and 'Logout' buttons.

Figure 3. – Screenshot of completed form to generate self-signed Root CA

- Confirm that you have received successful acknowledgement once the form has been completed

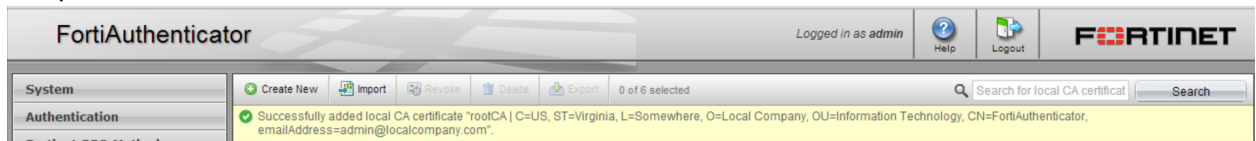


Figure 4. – Screenshot of successful acknowledgement of creation of root CA from FortiAuthenticator

<input type="checkbox"/>	rootCA	C=US, ST=Virginia, L=Somewhere, O=Local Company, OU=Information Technology, CN=FortiAuthenticator, emailAddress=admin@localcompany.com	C=US, ST=Virginia, L=Somewhere, O=Local Company, OU=Information Technology, CN=FortiAuthenticator, emailAddress=admin@localcompany.com	Active	Root CA
--------------------------	--------	--	--	--------	---------

Figure 5. – Entry of root CA in FortiAuthenticator

Creating a Local Services Certificate

In order for the FortiAuthenticator to use a certificate in mutual authentication (supported by EAP-TLS), a local services certificate has to be created on behalf of the FortiAuthenticator. This can be accomplished via the following steps:

- Navigate to “Certificate Management | End Entities | Local Services”

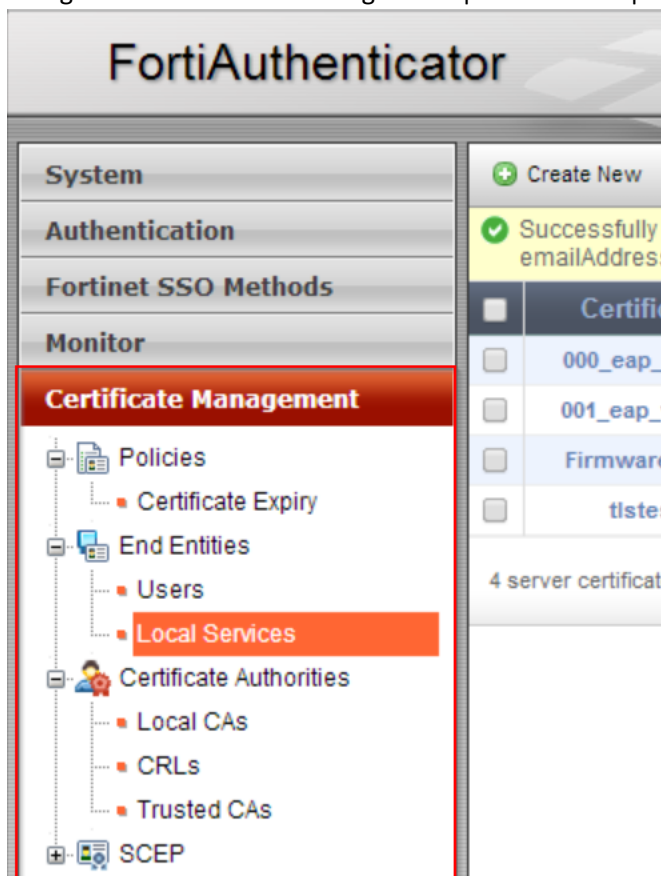


Figure 6. – Screenshot of “Local Services” location in FortiAuthenticator

- Click “Create New”

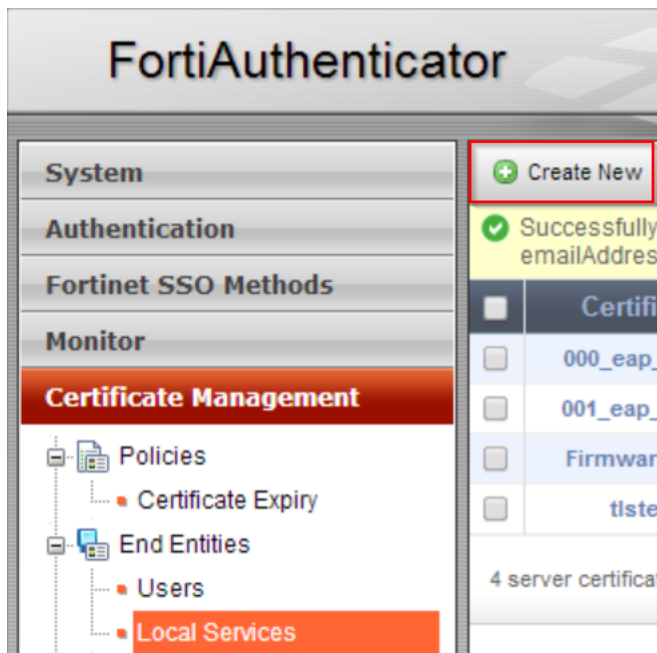


Figure 7. – Screenshot of “Create New” button for “Local Services”

3. Complete the information in the fields pertaining to your organization

 The screenshot shows the FortiAuthenticator web interface with the 'Create New' form for a 'Local Services' certificate. The form is titled 'Certificate ID: 000_eap_local_svc'. It has several sections:

- Certificate Signing Options:** Issuer is set to 'Local CA'. Certificate authority is set to 'rootCA | C=US, ST=Virginia, L=Somewhere, O=Local Company, OU=Information Technology, CN=FortiAuthenticator, emailAddress=admin@localcompany.com'.
- Subject Information:** Subject input method is 'Fully distinguished name'. Fields include: Name (CN): 'fortiauth-eap', Department (OU): 'Information Technology', Company (O): 'Local Company', City (L): 'Somewhere', State/Province (ST): 'Virginia', Country (C): 'United States (US)', and Email address: 'fortiauth-admin@localcom'.
- Subject Alternative Name:** Fields for 'Email' and 'User Principal Name (UPN)' are present.
- Additional Options:** Validity period is set to 'Set length of time' with a value of '1825' days. Key type is 'RSA' and key size is '2048 Bits'.

 The left navigation menu is visible, with 'Local Services' highlighted. The top right shows 'Logged in as admin' and 'Logout' buttons.

Figure 8. – Screenshot of completed form for “Local Services” certificate used by FortiAuthenticator

4. Confirm that the recently created certificate exists in the “Local Services” certificate list

 The screenshot shows the FortiAuthenticator web interface displaying a list of certificates. The table has columns: Certificate ID, Subject, Issuer, and Status. The first row shows the certificate '000_eap_local_svc' with subject 'C=US, ST=Virginia, L=Somewhere, O=Local Company, OU=Information Technology' and issuer 'C=US, ST=Virginia, L=Somewhere, O=Local Company, OU=Information Technology'. The status is 'Active'.

Certificate ID	Subject	Issuer	Status
000_eap_local_svc	C=US, ST=Virginia, L=Somewhere, O=Local Company, OU=Information Technology	C=US, ST=Virginia, L=Somewhere, O=Local Company, OU=Information Technology	Active

Figure 9. – Screenshot of the “Local Services” list

Configuring RADIUS-EAP on FortiAuthenticator

In order for the FortiAuthenticator to present the newly created “Local Services” certificate as its authentication to the client, the RADIUS-EAP must be configured to use this certificate. To do this, follow the procedure listed below:

1. Navigate to “Authentication | RADIUS Service | EAP”

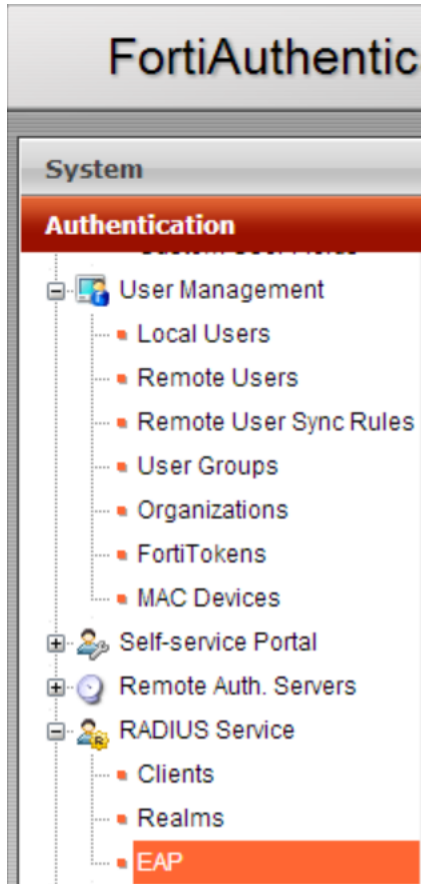


Figure 10. – Screenshot of the EAP section in FortiAuthenticator

2. Select the corresponding “Local Services” certificate in the “EAP Server Certificate” section | Choose the Local CA certificate previous configured in the “Local CAs:” section:

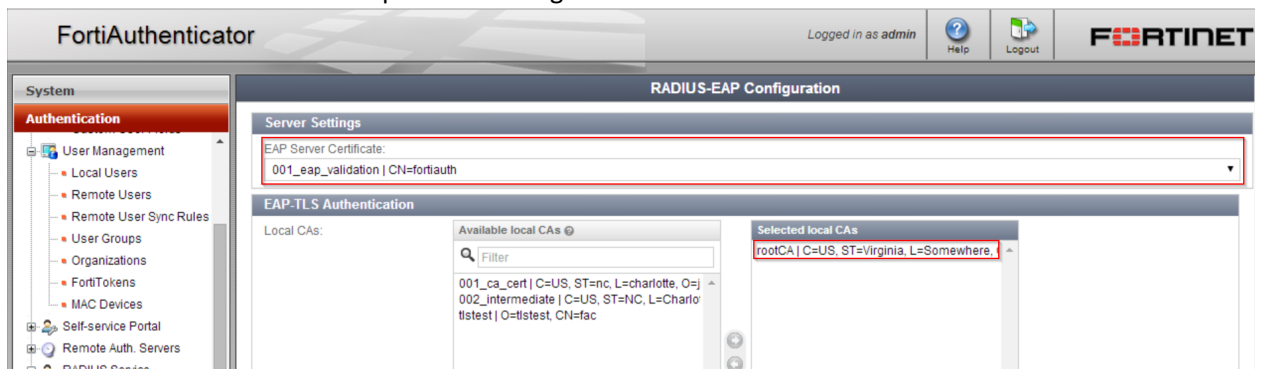


Figure 11. – Screenshot of EAP Services section

3. Click “OK” to save the configuration

Configuring RADIUS Client on FortiAuthenticator

The FortiAuthenticator has to be configured to allow RADIUS clients to make authorization requests to it. To do this, follow the procedure listed below:

1. Navigate to “Authentication | RADIUS Service | Clients”

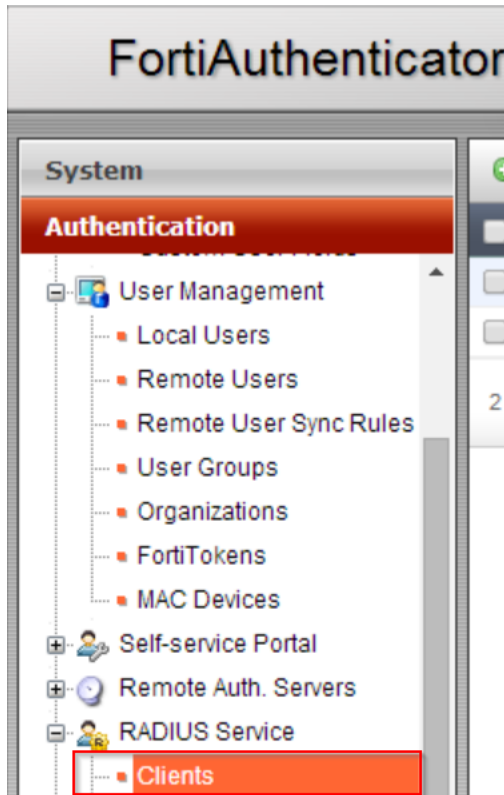


Figure 12. – Screenshot of “Clients” (RADIUS) in FortiAuthenticator

2. Click “Create New”

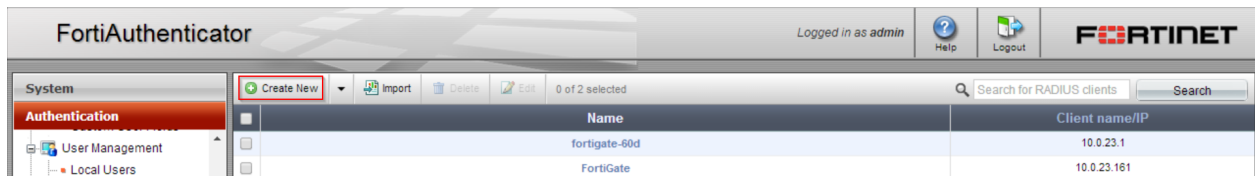


Figure 13 . – Screenshot of “Create New” button for the “Clients” (RADIUS) section in FortiAuthenticator

- Complete the applicable information for your RADIUS server (example in screenshot below):

Figure 14. – FortiAuthenticator RADIUS Client configuration screenshot

***Please Note: EAP-TLS is the only EAP type selected to prevent fallback to a less secure version of authentication if a certificate is not presented by the client"**

- Click "OK" to save the configuration

Configuring Local User on FortiAuthenticator

The authentication of the client will be tied to a user account on the FortiAuthenticator. In this scenario, a local user will be configured but remote users associated with LDAP can be configured as well. To configure a local user on the FortiAuthenticator, follow the procedure below:

- Navigate to "Authentication | User Management | Local Users"

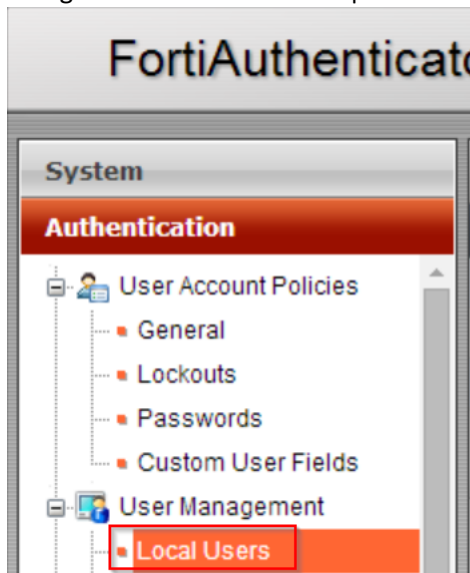


Figure 15. – Screenshot of "Local Users" section in FortiAuthenticator

2. Click “Create New”

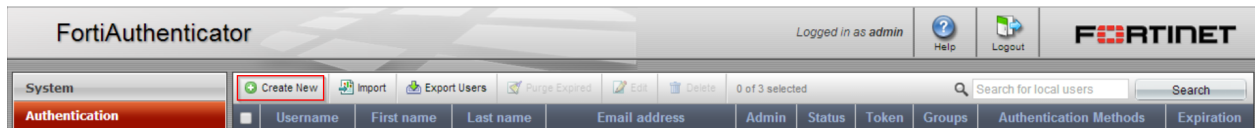


Figure 16. – Screenshot of “Create New” button for Local Users in FortiAuthenticator

3. Fill out applicable user information

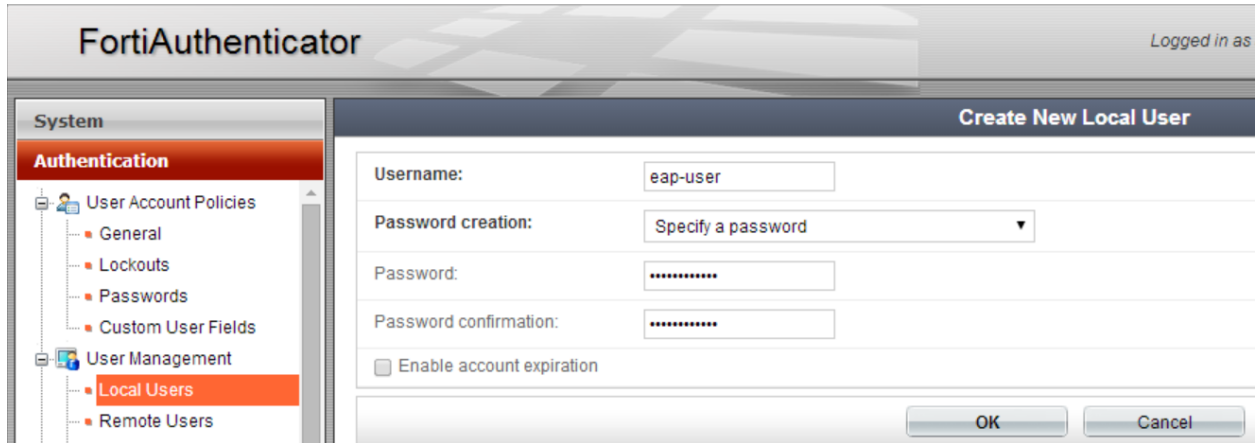


Figure 17. – Screenshot of “Create New Local User” on FortiAuthenticator

4. Click OK

Please Note: The default options set for the user are all that is needed for this particular scenario

Configuring End User Certificates on FortiAuthenticator

The certificate created locally on the FortiAuthenticator will be associated with the local user. It is important to note that the Common Name (CN) must match the username exactly of the user that is registered in the FortiAuthenticator (i.e. “eap-user” in this case). To create a corresponding certificate for the user, follow the steps below:

1. Navigate to “Certificate Management | End Entities | Users”

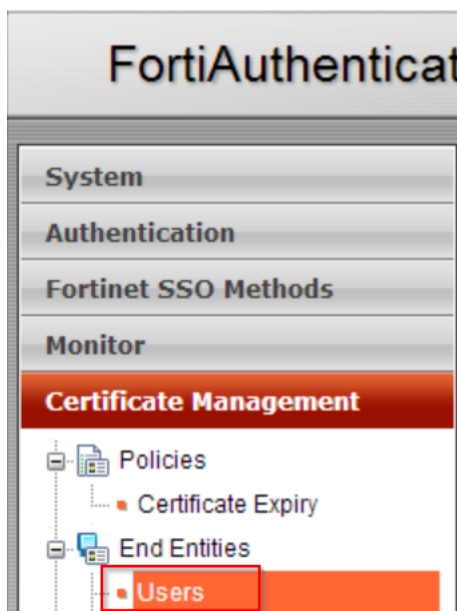


Figure 18. – Screenshot of the “Users” certificate section in FortiAuthenticator

2. Click “Create New”

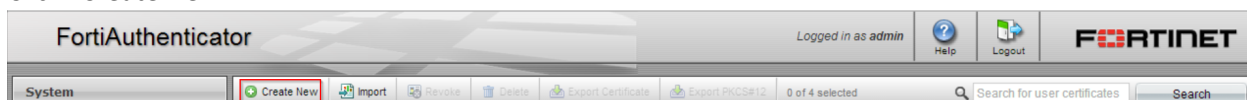


Figure 19. – Screenshot of “Create New” button in FortiAuthenticator

3. Fill in the applicable information to map the certificate to the correct user (example in screenshot below):

 The image shows the 'Create New User Certificate' dialog box. The left sidebar is expanded to show 'Certificate Management' > 'Users'. The main form has several sections:

- Certificate ID:** A text field containing '000_eap_user'.
- Certificate Signing Options:**
 - Issuer:** Radio buttons for 'Local CA' (selected) and 'Third-party CA'.
 - Local User (Optional):** A dropdown menu with 'eap-user' selected.
 - Certificate authority:** A text field containing 'rootCA | C=US, ST=Virginia, L=Somewhere, O=Local Company, OU=Information Technology, CN=FortiAuthenticator, emailAddress=admin@localcompany.com'.
- Subject Information:**
 - Subject input method:** Radio buttons for 'Fully distinguished name' (selected) and 'Field-by-field'.
 - Name (CN):** A text field containing 'eap-user'.
 - Department (OU):** A text field containing 'Corporate'.
 - Company (O):** A text field containing 'Local Company'.
 - City (L):** A text field containing 'Somewhere'.
 - State/Province (ST):** A text field containing 'Virginia'.
 - Country (C):** A dropdown menu with 'United States (US)' selected.
 - Email address:** A text field containing 'regularuser@localcompt'.
- Subject Alternative Name:**
 - Email:** A text field.
 - User Principal Name (UPN):** A text field.
- Additional Options:**
 - Validity period:** Radio buttons for 'Set length of time' (selected) and 'Set an expiry date'.
 - Days:** A text field containing '365'.
 - Key type:** A dropdown menu with 'RSA' selected.

Figure 20. – Screenshot of “New User Certificate” dialog on FortiAuthenticator

4. Confirm that certificate was successfully created

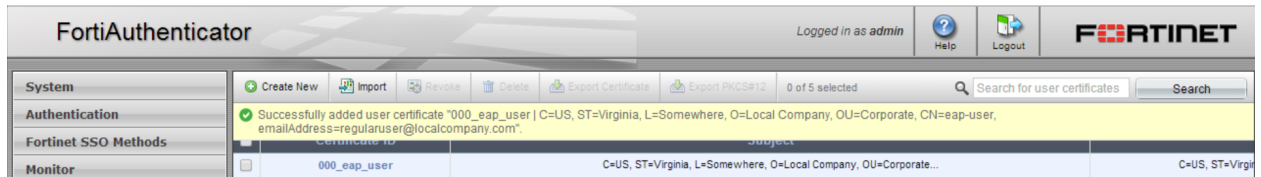


Figure 21. – Screenshot of newly created certificate in FortiAuthenticator

FortiGate

Creating RADIUS Client on FortiOS

In order to proxy the authentication request from the wireless client, the FortiGate will need to have a RADIUS server to submit the authentication request to. This is achieved by configuring a RADIUS server to be used in the FortiGate. To do this, follow the procedure listed below:

1. Log into FortiGate WebGUI with administrative user account
2. Navigate to “User & Device | Authentication | RADIUS Servers”

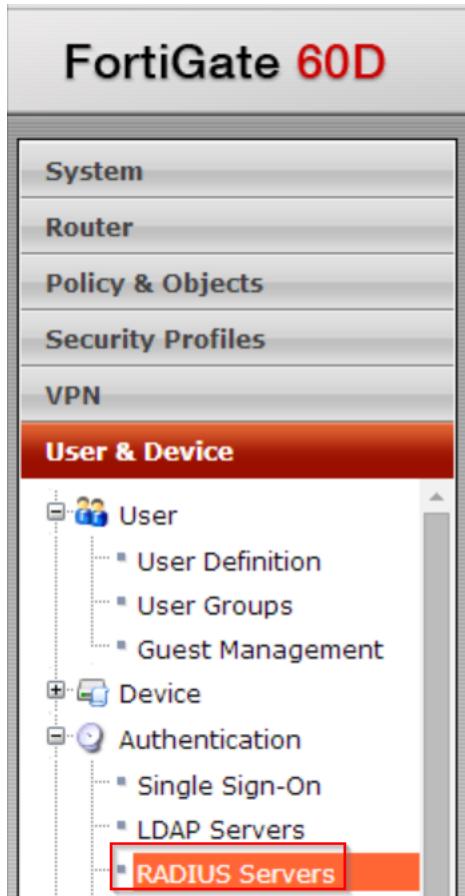


Figure 22. – Screenshot of “RADIUS Servers” section in FortiGate WebGUI

3. Click “Create New”
4. Complete the applicable information for the RADIUS server (example in screenshot below):

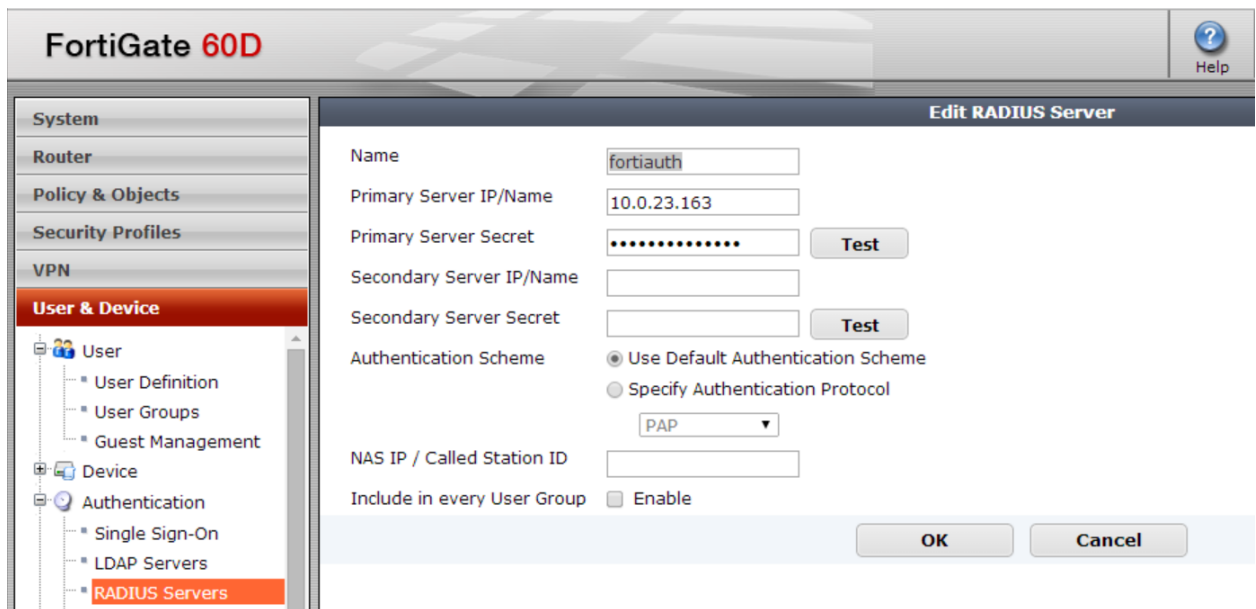


Figure 23. – Screenshot of RADIUS configuration on FortiGate WebGUI

5. Click “OK” to save the configuration

Creating WiFi SSID on FortiGate

In order for the client to connect using its certificate a SSID has to be configured on the FortiGate to accept this type of authentication. To configure this, follow the instructions listed below:

1. Navigate to “WiFi Controller | WiFi Network | SSID”



Figure 24. – Screenshot of SSID section in FortiGate WebGUI

2. Click “Create New”
3. Create the applicable WiFi settings (example shown in screenshot below):

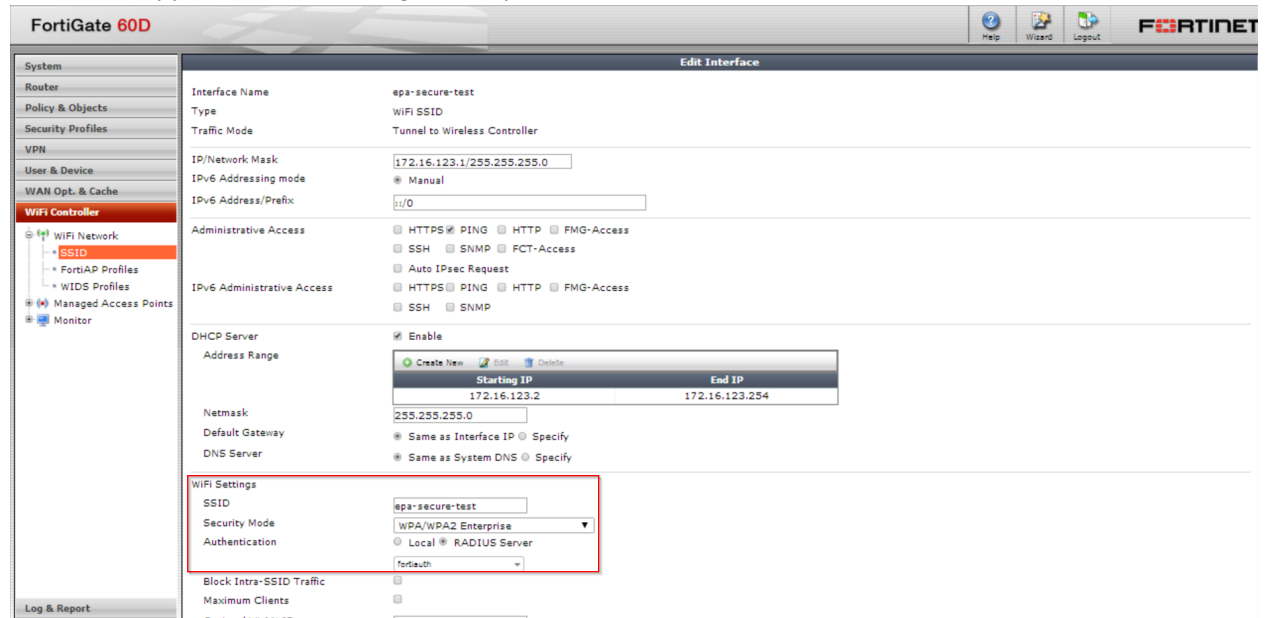


Figure 25. – Screenshot of WiFi configuration parameters in FortiGate WebGUI

Please Note: EAP-TLS is only supported in WPA/WPA2 Enterprise security mode

4. Click “OK” to save

Windows 7 PC Configuration

Exporting certificate from FortiAuthenticator

In order for the client to use the certificate for authentication to the FortiAuthenticator, the user certificate created in the FortiAuthenticator must first be exported. To do this, follow the instructions listed below:

1. Login to the FortiAuthenticator with administrative credentials
2. Navigate to “Certificate Management | End Entities | Users”

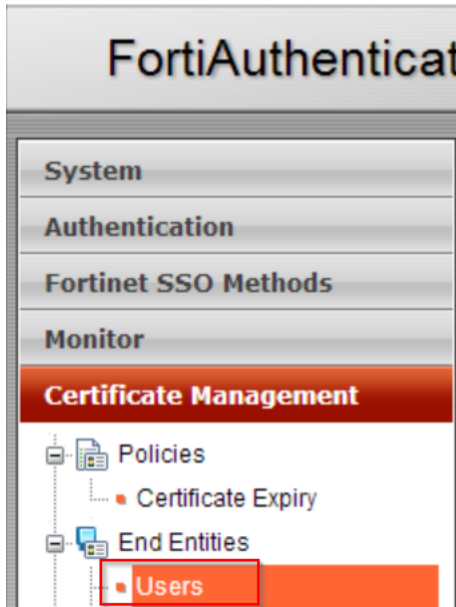


Figure 26. – Screenshot of the “Users” certificate section in FortiAuthenticator

3. Click the checkbox beside the certificate to import | Click “Export PKCS# 12”

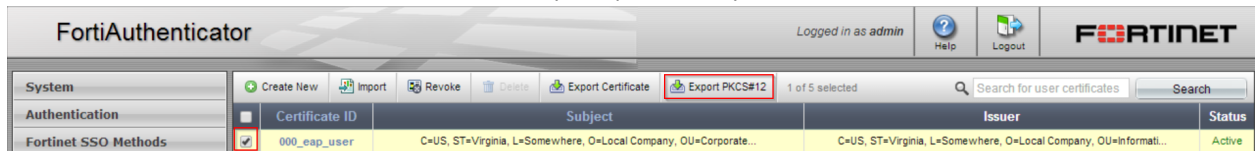


Figure 27. – Screenshot of export certificate button in FortiAuthenticator

4. In the “Export User Certificate and Key File” type a password in the “passphrase” (i.e. “fortinet”) that will be used when importing the certificate into Windows 7 PC

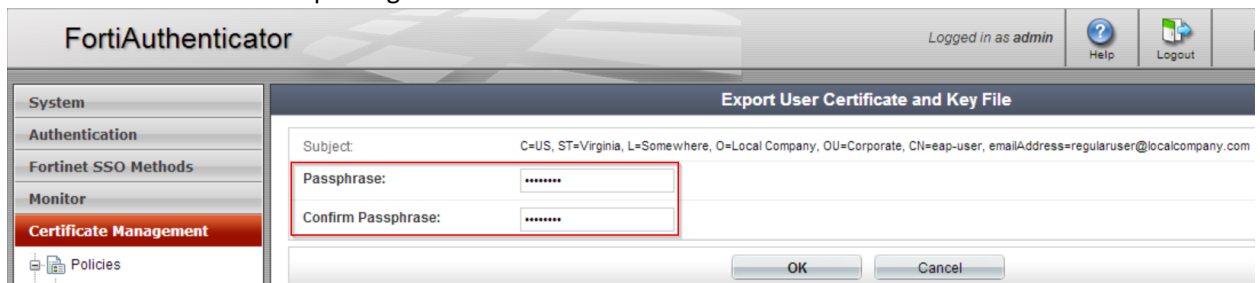


Figure 28. – Screenshot of passphrase in the “Export User Certificate and Key File” section of FortiAuthenticator

5. Click “OK”
6. Click “Download PKCS# 12 file” to pull this certificate local to your PC

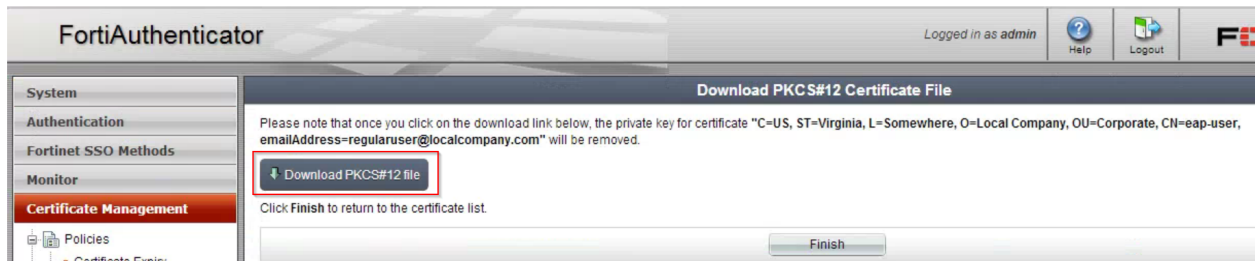


Figure 29. – Screenshot of the “Download PKCS# 12” certificate section on FortiAuthenticator

7. Click “Finish”

Importing certificate into Windows 7

Once the certificate has been exported, they can be imported to be used during authentication to the wireless. To do this, follow the instructions listed below:

1. On the Windows 7 PC, double-click the recently downloaded certificate from the FortiAuthenticator (this should launch the “Welcome to Certificate Import Wizard” as shown in the screenshot below:



Figure 30. – Screenshot of “Certificate Import Wizard”

2. Click “Next”

3. Make sure the correct certificate is shown in the “File Name” section in the “File to Import” page | Click “Next”

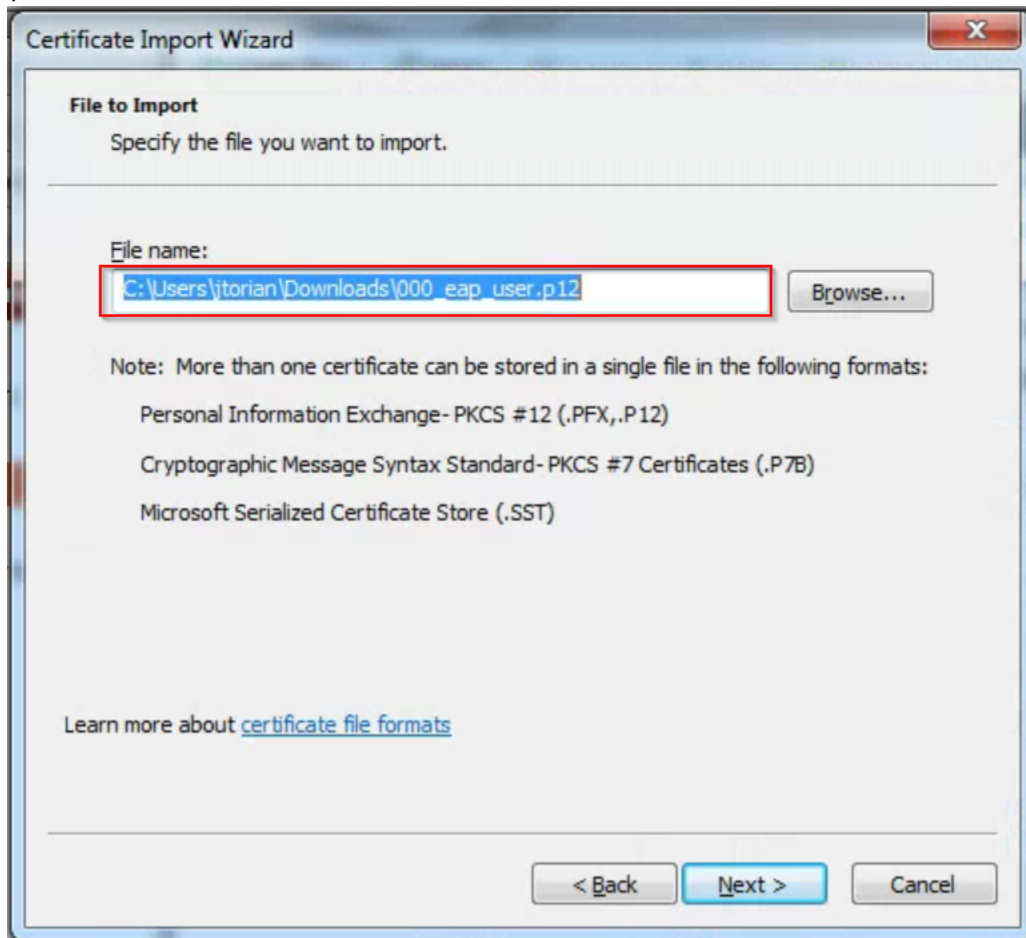


Figure 31. – Screenshot of the “File to Import” section

4. Type the “password” created on the FortiAuthenticator during the export of the certificate | Click “Mark this key as exportable” | Leave remaining defaults | Click “Next”

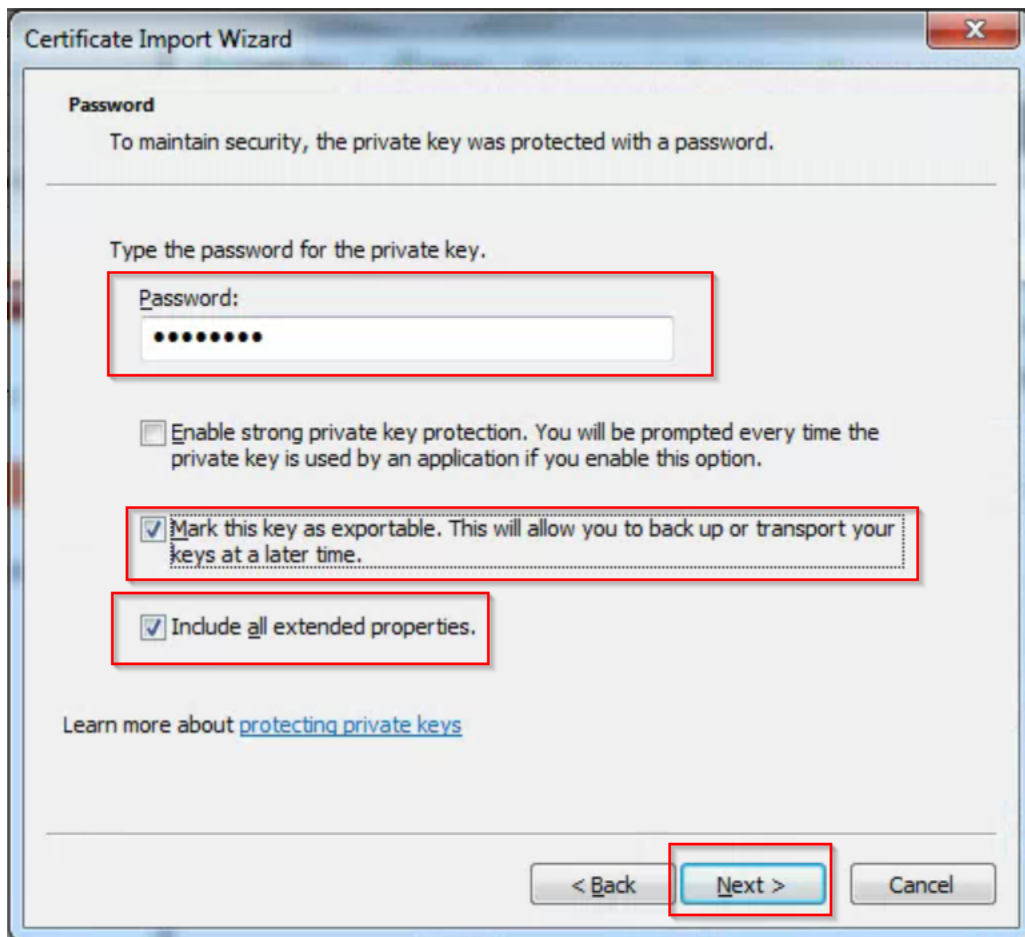


Figure 32. – Screenshot of the “password” section of the certificate import wizard

5. In the “Certificate Store” choose the “Place all certificates in the following store” | Click “Browse” | Choose “Personal” | Click “Next”

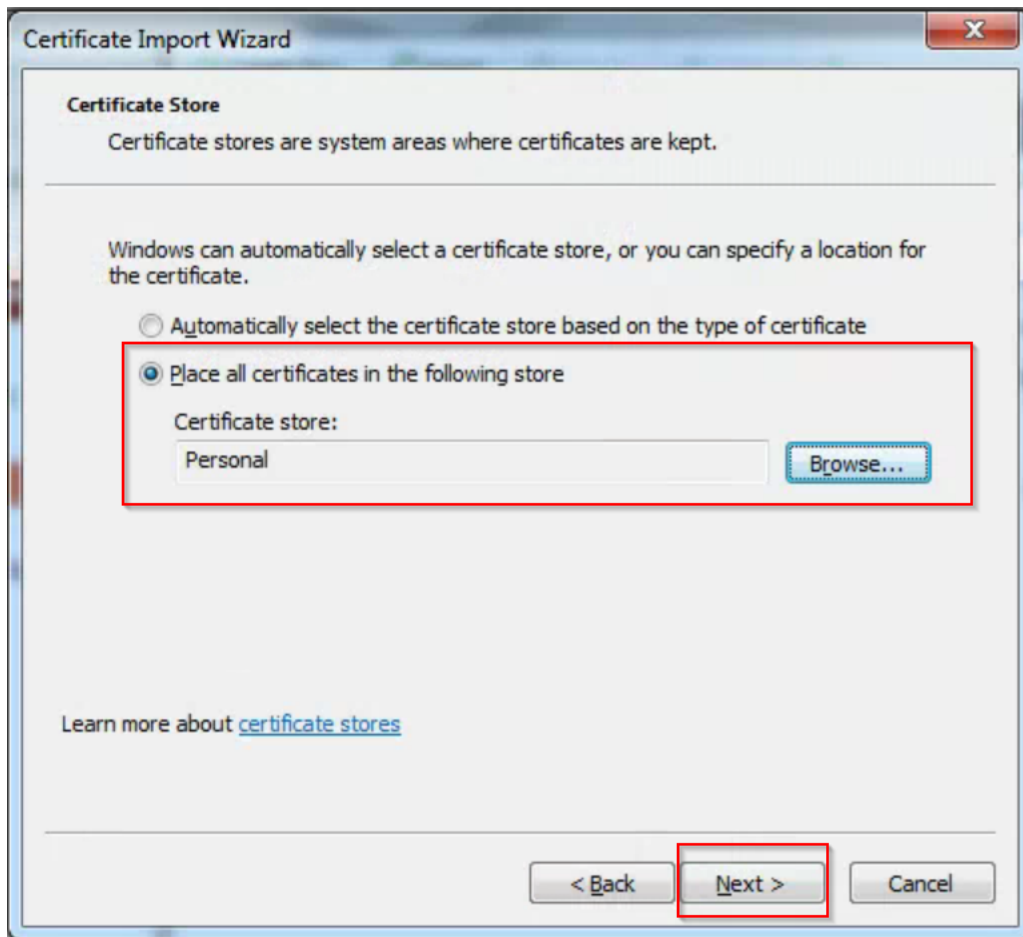


Figure 33. – Screenshot of “Certificate Store” section of the certificate import wizard

6. Click “Finish”

Please Note: You will get a dialog box to confirm if the certificate import was successful

Configuring Wireless Profile to use Certificate

After the certificate has been successfully imported into the Windows 7 PC, the wireless profile has to be configured to use this certificate when performing authentication. To do this, follow the instructions listed below:

1. Create a new wireless connection with the SSID of your wireless
2. Modify the newly created connection with the security configuration options shown in the screenshot below:

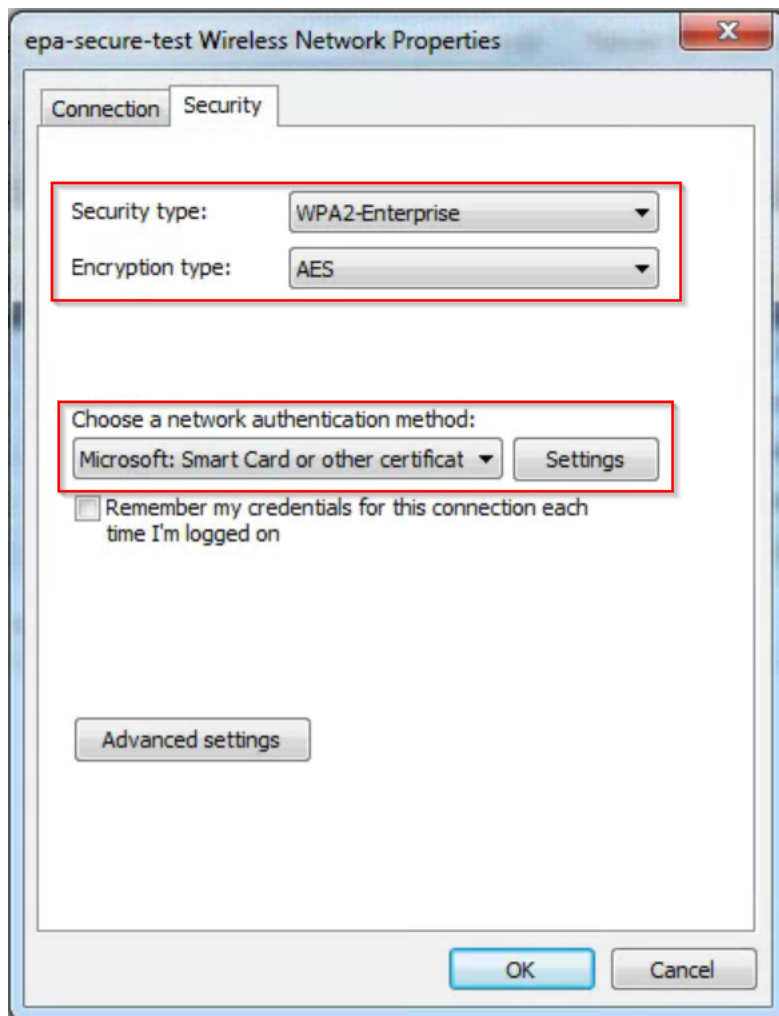


Figure 34. – Screenshot of Wireless Network properties for SSID

3. Click on “Settings” and set the configuration parameters shown in the screenshot:

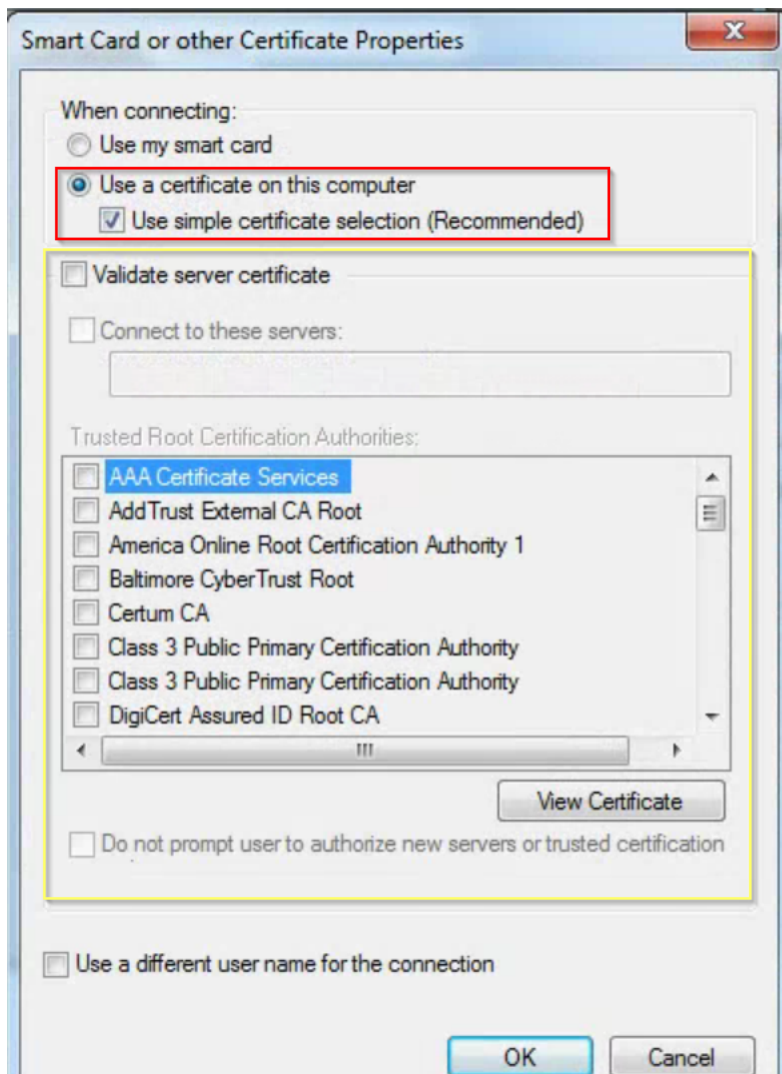


Figure 35. – Screenshot of the “Settings” configuration

***Please Note: For simplification purposes, the “Validate server certificate” has been disabled but EAP-TLS allows the client to validate the server as well as the server validate the client. To enable this, you will need to import the CA from the FortiAuthenticator to the Windows 7 PC and make sure that it is enabled as a “Trusted Root Certification Authority”.**

4. Click “OK”
5. Click “OK”

The configuration for the Windows 7 PC has been completed and the user should be able to authenticate to the wireless via the certificate without using username and password.

Appendix A: Verifying Login via FortiAuthenticator Logs

When the user attempts to authenticate to wireless using the certificate, they will have a specific log entry in the FortiAuthenticator. Below is a screenshot of the log entry displaying a valid logon attempt into the wireless from a client using a certificate for authentication.

The screenshot shows the FortiAuthenticator web interface. The top navigation bar includes 'System', 'Authentication', 'Fortinet SSO Methods', 'Monitor', 'Certificate Management', and 'Logging'. The 'Logging' section is expanded, showing a tree view with 'Log Access', 'Logs' (selected), 'Log Config', 'Log Setting', and 'Syslog Servers'. The main area displays a table of log entries. The selected entry (ID 33683) is highlighted in blue. A 'Log Details' pop-up window is open on the right, showing the following information:

Log Details	
ID	33683
Timestamp	Wed Jun 25 08:36:29 2014
Level	information
Action	Authentication
Status	Success
NAS Name/IP	10.0.23.1
Message	802.1x authentication successful
User	eap-user
Log Type	
Type Id	20420
Name	802.1x Authentication OK
Sub Category	Authentication
Category	Event
Description	802.1x authentication successful

Figure 36. – Screenshot of FortiAuthenticator logs showing successful authentication using certificate